

## NMAP der Security Port Scanner für Windows

Netzwerksicherheit vorbeugend - Befehlsreferenz

© 2002 by M.Rogge

Es gibt ihn schon lange, den Security Scanner von Fyodor mit dem aller bestens bekannten Namen NMAP.

NMAP heisst ausgeschrieben Network-Mapper.

Nun ist es endlich soweit und der Scanner ist in einem Projekt auch für Windows inklusive Installer verfügbar und bietet nun auch den Administratoren, die ausschließlich mit Windows arbeiten ein hervorragendes Tool.

Der Security Scanner soll Schwachstellen in einem Netzwerk aufzeigen, um vorbeugende Maßnahmen zur Security zu ergreifen.

Für die meisten Angriffe ist es jedoch immer erforderlich, dass man den Host kennt, dass man die dortigen Dienste kennt und welche Zugriffe möglich wären.

Bei einem Scanning kann man bereits unbemerkt sehr viele Informationen des Rechners erhalten der gescannt wird.

Das Tool NMAP bietet neben den einfachen Scans auch tiefere Scannmöglichkeiten, die einzelne Hosts ansprechen können um die dort arbeitenden Dienste heraus zu finden.

Sehr nützlich also scheint NMAP für Systemadministratoren zu sein, um die eigene Netzwerkstruktur auf mögliche Sicherheitsmängel zu scannen.

Für das genaue arbeiten mit NMAP sollte man sich mit Netzwerken, deren Struktur und TCP/IP auskennen, um entsprechende Befehle zu realisieren und die Ergebnisse auszuwerten.

Die derzeitigen Versionen von NMAP kann man auf den offiziellen Seiten bekommen, für WindowsXP sowie Windows2000 ist es derzeit die Version 1.3.0 und basiert auf der Version 2.54 Beta für Linuxsysteme.

Windows NMAP für WindowsXP/2000.

Linux NMAP für diverse Distributionen.

Was genau kann NMAP und wie kann ich vorgehen?

Die absolute Vielfältigkeit von NMAP macht es zu einem Programm, dass in keinem Werkzeugkasten eines Systemadministrators fehlen darf und sollte!

Sie erhalten nun einen Einblick in die Technik von NMAP und wie Sie konkret mit welchen Parametern arbeiten können.

### **Parameter und deren Bedeutung im Umgang mit NMAP**

Mit dem Parameter `-sP` kann man mit den Ping-Befehl aktive Hosts in einem Netzwerk erkennen, da hierbei ein ICMP-Echo Paket an das Zielhost gesendet wird, dass dann mit einem ICMP-Echo-Reply antwortet.

NMAP hat hierbei jedoch nur die Möglichkeit, "normale" Ping an einen Host zu senden.

Durch den Parameter `-sT` wird ein TCP Port Scan durchgeführt.

Zwangsläufig muß dabei eine Verbindung zum Zielhost aufgebaut werden, wobei das Prinzip des 3-Wege-Handshakes durchgeführt wird.

Das bedeutet im einzelnen, daß bei TCP Verbindungen nach dem Drei-Wege-Handshake-Prinzip ACK-Anfragen (ACK=Acknowledgement) an den anzugreifenden Host gesendet werden.

Als erstes werden dabei die SYN Pakete an den Server gesendet.

Der Server antwortet dann wie beschrieben mit SYN-ACK Paketen und erwartet dann eine Bestätigung durch ein ACK Paket vom Client.

Der Parameter `-sS` führt einen so genannten halboffenen Scan durch.

Ein Scan mit diesem Parameter wird deshalb so genannt, weil man keine vollständige TCP Verbindung aufbaut sondern lediglich eine SYN Anfrage an einen Host sendet.

Antwortet der Host dann mit einem SYN-ACK Paket kann man davon ausgehen, dass der Host listening erreichbar ist.

Durch die Rückgabe von so genannten RST-ACK Paketen kann man dann davon ausgehen, dass keine vollständige Verbindung zustande kommt.

Besonders interessant ist diese Scan-Methode da diese nicht so schnell erkannt werden kann.

Durch den Parameter `-sU` wird mit NMAP ein reiner UDP-Scan ausgeführt. Bei diesem Scan sollte im Normalfall angenommen werden, dass ein ICMP Paket als Antwort erscheint und unreachable erscheint. Das bedeutet, dass der Zielhost auf diesem Port nicht erreichbar ist. Folglich kann man von einem offenen Port ausgehen, wenn kein ICMP Antwort Paket ausgegeben wird.

### Weitere Parameter in Kurzform:

Parameter `-sF` für einen STEALTH-FIN-Scan bei dem RST Pakete zurück gegeben werden müssen wenn diese Ports geschlossen sind.

Parameter `-sX` trifft für einen vergleichbaren Scan zu. Hierbei wird ein Host mit FIN-Paket, ein URG-Paket und ein PUSH-Paket gescannt, wobei ebenfalls RST Pakete für geschlossene Ports zurück gegeben werden.

Parameter `-sN` führt einen TCP-Null-Scan durch. Bei dieser Art des Scans werden alle Flaggen geschlossen und das Zielsystem gibt RST Pakete als Antwort auf geschlossene Ports zurück. Diese Art von Scan ist fast nur bei Unix / Linux ausführbar!

Parameter `-PT`  
Mit einem TCP Ping können erreichbare Maschinen ermittelt werden, auch wenn ein Firewall ICMP Pings oder Echos blockiert werden. Hierzu verwendet diese Scan-Methode ein TCP Paket mit ACK (Empfangsbestätigung). Ist die Zielmaschine ansprechbar, antwortet sie mit einem RST (zurücksetzen). In der Regel wird hierzu der Port 80 benutzt, da er nur sehr selten von Firewalls gefiltert wird.

Parameter `-PS`  
Diese Option sendet SYN-Pakets, also eine Aufforderung zum Verbindungsaufbau, statt eines Pakets mit ACK (Empfangsbestätigung). Hier antwortet der Zielrechner mit einem RST (zurücksetzen) und es wird klar, der Rechner ist vorhanden und ansprechbar.

Parameter `-PI`  
Die PI-Option sendet einfach nur Pings und hofft auf Server, die ansprechbar sind und im eigenen Netz auch nach Broadcast Adressen suchen. Dies sind IP Adressen, die von außen erreichbar sind und Broadcasts (es wird kein festes Ziel definiert sondern an alle im Netz befindlichen Rechner gesendet) bei ankommenden IP Paketen absenden. Sollte dies der Fall sein, sollte das Loch schnell beseitigt werden, denn der PI Scan kann eine erste Vorbereitung zu einer Denial of Service Attacke sein. Genauer gesagt handelt sich hierbei fast immer um einen Smurf Angriff.

Parameter `-PB`  
Diese Option stellt den Default-Ping dar. Er verwendet sowohl ACK- wie auch ICMP Pakets parallel. Auf diese Weise können Firewalls überwunden werden, die nur eins von beiden filtern.

Parameter `-O`  
Diese Option aktiviert die Identifikation des Zielrechners über einen TCP/IP-Fingerabdruck. Sie benutzt dazu eine Reihe von Techniken, die die notwendigen Informationen aus dem Netzwerk-Stack des Zielrechners ziehen und diese Informationen dann mit denen in einer Datenbank mit bekannten OS-Fingerabdrücken vergleichen.

Parameter `-I`  
Mit der Option I lässt sich die TCP-Rückkennungs-Abtastung aktivieren. Aufgrund eines Bugs im Kennzeichnungsprotokoll (RFC 1413) erfolgt über das Protokoll die Freigabe des Usernamens, der jedem Prozess angefügt ist, der eine TCP-Verbindung aufgemacht hat.

Parameter `-f`  
Die Option f verursacht die benötigten SYN- FIN oder NULL Pakets zur Nutzung von fragmentierten IP-Pakets.

Verfolgt werden soll hierbei , TCP-Header auf mehrere kleine Pakete zu verteilen, um sie schwerer sichtbar zu machen.

Je nach eingesetzter Firewall oder auch Intrusion Detection System, können solche Pakete nicht erkannt werden oder nur schwer, da diese fragmentiert sind und verteilt.

Vergleichbares Vorgehen eines verteilten Angriffes mit fragmentierten IPs.

Parameter -oN

Mit der Option -oN können die Scan-Ergebnisse in eine Datei geschrieben werden.

Diese Funktion ist nicht uninteressant, wenn man die Ergebnisse fachgerecht auswerten möchte, was für Systemadministratoren durchaus relevant sein dürfte.

Parameter -p

Mit der Option -p lassen sich Folgen von zu scannenden Ports oder einen Bereich von zu scannenden Ports angeben.

Parameter -D

Die Option -D ist besonders interessant, denn mit dieser Option können weitere Maschinen als so genannte Lockvögel eingesetzt werden, die alle den gleichen Zielrechner scannen.

Auch wenn an der Zielmaschine die Abtastversuche registriert werden, kann in der Regel keine Zuordnung erfolgen, von wo aus der tatsächlich echte Scanversuch startete.

Parameter -S

Mit der Option -S können gesendete Pakets gespoofed, also mit einer falschen Absender IP-Adresse versehen werden.

Auch wenn die Schutzsysteme des Zielrechners Scans registrieren, können Sie ihn nicht zum Ursprung zurückverfolgen.

Parameter -g

Die Option -g setzt einen Quellport in die verschickten Pakets.

Viele schlecht administrierte & naive Firewalls und Paketfilter bilden eine Ausnahme in ihren Filterregeln, erlauben DNS (53) und FTP-Data ( 20) Pakets und akzeptieren eine Verbindung.

Dieser Umstand führt die Sicherheit ad absurdum, denn Angreifer markieren den Zugriff als DNS oder FTP und verändern darunter ihren Quellport.

Parameter -r

Diese Option gibt NMAP die Anweisung, bis zu 2048 zufällige Maschinen für einen Scan zu benutzen, um die Sicherungssystem der eigentlichen Zielmaschine zu verwirren.

Besonders dann, wenn diese Option mit anderen Optionen zum Verlangsamen des Timings der Scans kombiniert wird.

Kombiniert man als Beispiel die Option -D-r dürfte dieser Scanlauf interessant sein :)

Parameter -m

Mit der Option -m (max sockets) lässt sich die Höchstzahl der Sockets einstellen, die parallel benutzt werden.

Diese Option wird gerne dazu benutzt, um die Scans langsamer zu machen und zu verhindern, dass die Zielrechner abstürzen.

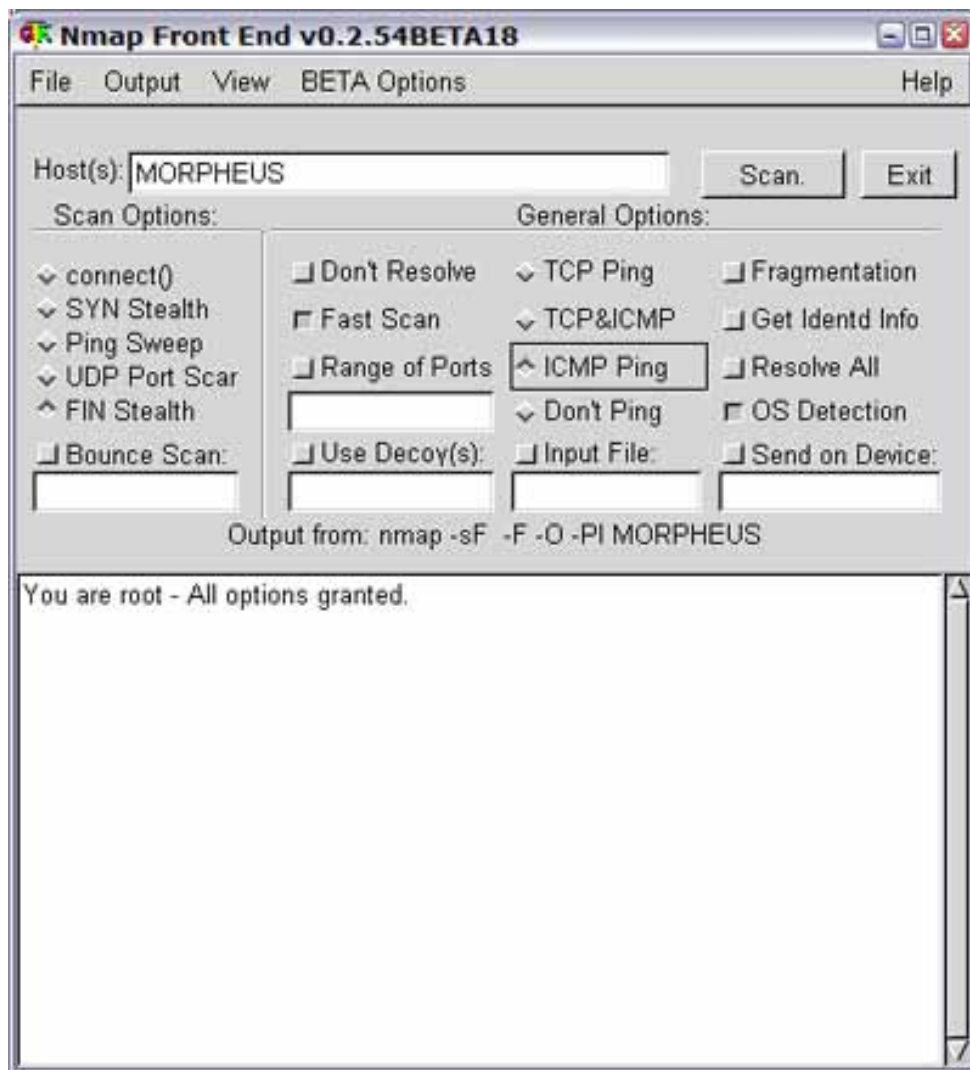
NMAP ist an sich schon ein Werkzeug, mit dem Scans weitestgehend unentdeckt bleiben.

Man nennt es in Fachkreisen auch Stealth.

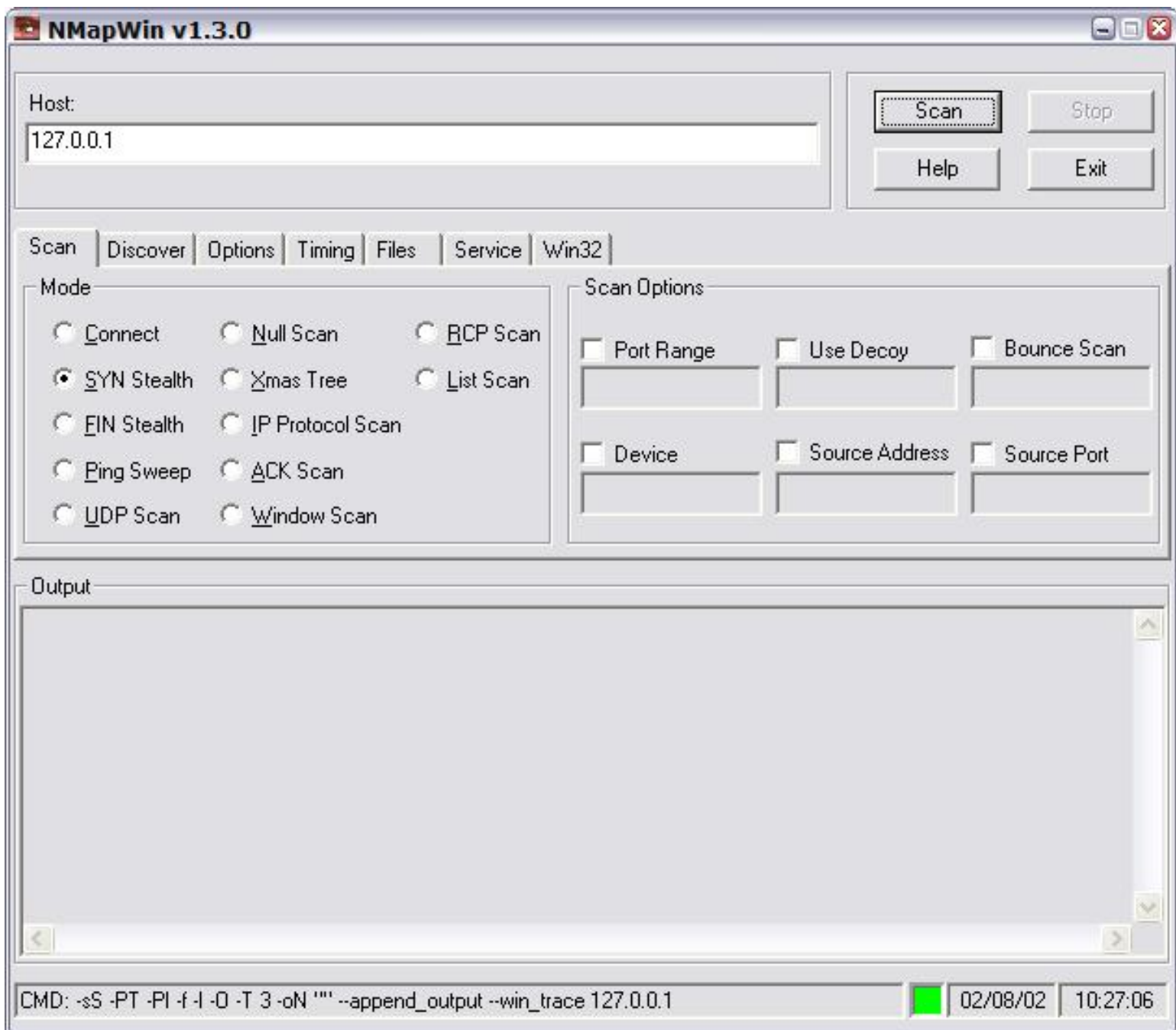
In einigen Fällen kann aber mit zusätzlichen Optionen das Timing noch feiner abgestimmt werden.

Parameter -T (Paranoid, Sneaky, Polite, Normal, Aggressive, Insane)

Mit den -T Optionen lässt sich das Timing der Scans passgenau auf das Zielsystem einstellen.



Als wichtige Anmerkung erscheint mir jedoch, daß bei fast allen Scanarten root erforderlich ist und ein Linux System die Performance eines ausführlichen Scan mit NMAP wesentlich steigert. Ach bei Windows Betriebssystemen, auf denen NMAP zum Einsatz kommen soll gilt das root Recht. Also muss man unter Windows mindestens Computeradminstrator Zugriffsrecht haben. Da NMAP auch als 32Bit Version für diverse Windows Betriebssysteme erhältlich ist, sollte man dort besonders auf eine starke Rechenleistung setzen. Empfehlenswert ist Windows nicht, um es als Scan Basissystem für einen derart umfangreichen Scanner wie NMAP zu verwenden.



Hier kann man schön erkennen, welche Befehle NMAP als Kommando ausführen würde, da ein solches Frontend normal nicht vorgesehen ist.

Die Frontends zwischen Linux (oberes Bild) und Windows (unteres Bild) unterscheiden sich nicht merklich voneinander.

Mit nmap für Windows wird ebenfalls WinPcap geliefert. (Windows Packet Library)

Ein Download und weitere Informationen erhalten Sie [hier](#).

Die aktuell mitgelieferte WinPcap Version bei WindowsNMAP ist Version 2.3.

Sie sehen schon, NMAP ist durchaus ein sehr vielseitiger Scanner und beinhaltet Techniken, die wir bereits aus Angriffsszenarien kennen.

Systemadministratoren sollten sich mit NMAP vertraut machen und sich regelmässig damit die Arbeit im Netzwerk erleichtern, um zusätzliche Sicherheitsmaßnahmen ergreifen zu können.

Alle Downloads und weitergehende Infos:

[Windows NMAP](#) für WindowsXP/2000.

[Linux NMAP](#) für diverse Distributionen.

[WinPcap](#) für Windows Version 3

Informationen zu NMAP/NetworkMapper finden Sie auf [Computec.ch](#)

**Danke für die Hilfe und Realisierung bei Holger & Udo.**

**Fragen, Kritik oder Anregung: EMail [mr@brain-pro at de](mailto:mr@brain-pro.de)**

**Best Regards & Greetings**

**M.Rogge // [www.brain-pro.de](http://www.brain-pro.de)**

**Berichte dieser Seite sind in guter Absicht und mühsamer Arbeit erstellt worden, daher möchte ich Sie bitten keine Anleitung und/oder andere Texte frei zu kopieren.**

**Unter Angabe des Autors und der URL sowie eine Benachrichtigung per E-Mail ist eine weitere Veröffentlichung jederzeit möglich.**

**Für einen Missbrauch zeichnet sich der Autor nicht verantwortlich, da eine kriminelle Handlung oder vergleichbares Handeln nicht damit unterstützt werden soll!**